Immediate Actions for CAFT Originators (Servus Business Members) - Password Reset, Daily File Reviews, Best Practices to Stay Cyber Aware

Updated: November 6, 2023

1. Reset CAFT Passwords

To keep your CAFT credentials such as user IDs and passwords safe and secure, all CAFT users **must reset user passwords immediately, if you haven't already**:

- Login to CAFT by entering the following URL directly into the address bar of your browser: https://www.caft.paymentsanytime.com
- Double-check the URL is correct before entering your existing credentials.
- Create a new and unique CAFT password:
    - To create a new password, select the "Self-service" option on the CAFT login screen OR click on "Manage my password" on the CAFT main menu once you've logged in.
    - You can also request a reset of your CAFT user password by contacting Servus's Business Services team at BusinessServices@servus.ca. Please be prepared to authenticate your identity.
- CAFT users should update their passwords frequently. The CAFT system provides a password change notification every 60 days. Best practice for password security includes: minimum of 8 characters; and a unique and complex combination of numbers and upper- and lower-case letters.

2. In your CAFT File History, review files submitted since October 31, 2023

Take advantage of the temporary one-day hold placed on AFTs by PPJV to identify suspicious files or transactions each day that you may want to remove from processing.

- If you see a suspicious or fraudulent transaction on your account, contact your Servus Cash Management Relationship Manger or Analyst immediately. In your email, please include the originator name and number, file number, dollar value and payee name of all suspicious items contained within the file.
- If you notice a file has been sent that you have not authorized, review in detail including reviewing your Servus account. You can also review the CAFT Change Report for any changes that may have been made that you did not complete, which would be an indicator of potential fraud. Additionally, if advised by a recipient that funds were not received, review the file details immediately for potential changes not made by you.

3. **Best Practices for Securely Accessing CAFT**

- **Ensure you are accessing the legitimate CAFT Payment Services website.** The best way to do this is to visit/logon to the CAFT system directly from the web address: https://www.caft.paymentsanytime.com.
    - **Save the above web address as a favorite**. This way you can ensure that you are always accessing the legitimate PPJV CAFT website, avoiding potential phishing attempts.
- **NEVER click on a link to CAFT sent via an unexpected email, text message or from a search engine advertisement.** Pay close attention to link URLs and NEVER access the system by following links in e-mails, SMS/text messages, or other messaging platforms. Never follow Google ads or other online advertising links to access the site. These methods can lead you to fraudulent sites which can appear legitimate.
- **Activate features built into the CAFT system** that help mitigate risk—such as establishing limits on transaction and file amounts.
- **Educate your CAFT users** on appropriate steps.
- Note that Servus Branches are required to **follow authentication processes** when a password reset is requested.

4. **Questions?** Contact BusinessServices@Servus.ca